I. J. Computer Network and Information Security, 2012, 2, 36-42
Published Online March 2012 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2012.02.06

A Novel Security Scheme for Secret Data using Cryptography and Steganography

Phad Vitthal S., Bhosale Rajkumar S., Panhalkar Archana R.

Department of Computer Engineering, Pravara Rural Engg. College, Loni, M.S., India
phadvs@gmail.com, bhos_raj@rediffmail.com, archana10bhosale@rediff.com

***Abstract*—With the development of network techniques the problem of network security becomes more and more important. The use of Word Wide Web has grown extremely in the past few years. Furthermore, many end users can easily use tools to synthesize and edit multimedia information. Thus, security has become one of the most significant problems for distributing new information technology. It is necessary to protect this information while communicated over insecure channels. Thus, a need exists for developing technology that will help protect the integrity of digital content and secure the intellectual property rights of owners. Cryptography and Steganography are the two major techniques for secret communication. The contents of secret message are scrambled in cryptography, where as in steganography the secret message is embedded into the cover medium. In this proposed system we developed high security model by combining cryptographic and Steganographic security. In cryptography we are using advanced encryption standard (AES) algorithm to encrypt secret message and then pixel value differencing (PVD) with K-bit least-significant-bit (LSB) substitution is used to hide encrypted message into truecolor RGB image. Our proposed model gives two tier security to secret data. Further our proposed method gives high embedding capacity and high quality stego images.**

***Index Terms* - Cryptography, Advance encryption standard (AES), Steganography, Pixel-value differencing (PVD), Least-significant-bit (LSB) substitution.**

I. INTRODUCTION

The applications accessing multimedia systems and content over the web have grown extremely in the past few years. The digital information revolution caused significant changes in the global society. In recent year, Internet multimedia applications have become very popular. Valuable secret information is vulnerable while in storage and during transmission over a network by unauthorized access. In this age of universal electronic connectivity, of viruses and hackers, of electronic eavesdropping and electronic fraud, there is indeed a need to protect information from passing before curious eyes or, more importantly, from falling into wrong hands. Thus, multimedia security is much to consider in distributing digital information safety. Cryptography and Steganography are two important branches of information security. Cryptography provides encryption techniques for a secure communication. Cryptography is the science that studies the mathematical techniques for keeping message secure and free from attacks [1],[2]. Steganography is the art and science of hiding communication [3]. Steganography involves hiding information so it appears that no information is hidden at all. The least-significant bit (LSB) insertion method, which uses fixed *K*- LSBs in each pixel to embed secret message, is the most common and easy one to hide message in an image [4]. However, it is easy to reveal a

Copyright © 2012 MECS

stego-image produced by the LSB insertion method. Image steganography has many applications, especially in today's modern, high-tech world. Steganography have many advantages but it have some limitations also [5]. Privacy and secrecy is a concern for most people on the internet. Image steganography allows for two parties to communicate secretly and covertly.

In this paper we will focus to develop a high security model for secret data, which uses both cryptography and Steganography. Advanced encryption standard(AES) is used for encryption [6],[7]. AES is a symmetric-key block cipher having high efficiency with respect to security, speed. Encrypted secret message is embedded in truecolor RGB image by using pixel value differencing (PVD) and K-bit least-significant-bit (LSB) substitution [8]. In PVD method the difference between the two consecutive pixels in the cover image is used to determine what size the secret message is to be hidden. A small difference value can be located on a smooth area and the large one is located on an edged area. Pixels located in edge areas are embedded by *K*- bit LSB substitution method with a larger value of K than that of the pixels located in smooth areas. This steganography method provided the stego-image has an imperceptible quality.

We discuss literature survey in Section II. In this section we give overview of cryptography, advanced encryption standard(AES), steganography, pixel value differencing (PVD) and K-bit least-significant-bit (LSB) substitution. Proposed method is described in section III which consists of data embedding algorithm and data extraction algorithms. Experimental results are described in section IV. We measure data hiding capacity in terms of bits and peak signal-to-noise ratio (PSNR) is used to evaluate qualities of the stego images which is described in section IV. Section V draws a conclusion.

II. RELATED WORK

There are many aspects to security and many applications. One essential aspect for secure communications is that of cryptography. Cryptography is technique for keeping message secure and free from attacks. In cryptography secret message is scrambled. Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication [2]. Communication security of data can be accomplished by means of standard symmetric key cryptography. Such important data can be treated as binary sequence and the whole data can be encrypted using a cryptosystem. It has been many years research to encryption technology, there are many encryption algorithms.

The three types of algorithms are described:

1) Symmetric Algorithm or Private Key
   Uses a single key for both encryption and decryption.
2) Asymmetric or public key Algorithm
   Uses one key for encryption and another for decryption
3) Hash Functions: Uses a mathematical transformation to
   irreversibly "encrypt" information.

Steganography is the other technique for secured communication [3]. Steganography involves hiding information so it appears that no information is hidden at all. If a person or persons views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information. Steganography is the process of hiding a secret message within cover medium such as image, video, text, audio [9].

Image steganography has many applications, especially in today's modern, high-tech world. Privacy and secrecy is a concern for most people on the internet. Image steganography allows for two parties to communicate secretly and covertly. It allows for some morally-conscious people to safely whistle blow on internal actions; it allows for copyright protection on

Copyright © 2012 MECS

digital files using the message as a digital watermark. One of the other main uses for image steganography is for the transportation of high-level or top-secret documents between international governments

Steganography systems can be grouped by the type of covers used (graphics, sound, text, executables) or by the techniques used to modify the covers.

1) Substitution system [15]
2) Transform domain techniques [16]
3) Spread spectrum techniques [17]
4) Statistical method [18]
5) Distortion techniques [19]
6) Cover generation methods [19]

A. Advanced Encryption Standard (AES)

Advanced Encryption Standard is the Rijndael algorithm by two researchers Dr. Joan Daemon and Dr. Vincent Rijmen from Belgium [6],[7]. Unlike its predecessor, DES, AES does not use a Feistel network [10]. The AES algorithm is a symmetric key block cipher with a block length of 128 bits and support for key lengths of 128, 192, and 256 bits. The AES algorithm is a symmetric key algorithm which means the same key is used to both encrypt and decrypt a message. Also, the cipher text produced by the AES algorithm is the same size as the plain text message. Most of the operations in the AES algorithm take place on bytes of data or on words of data 4 bytes long, which are represented in the field $GF(2^8)$, called the Galois Field. AES is based on a design principle known as a Substitution permutation network. AES operates on a 4×4 matrix of bytes, termed the *state* . The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key. The AES algorithm loops through certain sections N_r times.

It is fast in both software and hardware.

AES Algorithm have following steps.

1) KeyExpansion—Round keys are derived from the cipher key using Rijndael's key schedule.
2) Initial Round
   a) AddRoundKey—each byte of the state is combined with the round key using bitwise XOR.
3) Rounds
   a) SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
   b)ShiftRows—A transposition step where each row of the state is shifted cyclically a certain number of steps.
   c)MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
   d)AddRoundKey
4) Final Round (no MixColumns)
   a) SubBytes
   b) ShiftRows
   c) AddRoundKey

Advantages of using AES algorithm

1) Very Secure.
2) Reasonable Cost.
3) Main Characteristics
   i) Flexibility, ii) Simplicity

B. PVD and K-bit LSB Steganography

In pixel-value differencing (PVD) stegnography method first, the cover image is partitioned into nonoverlapping blocks with two consecutive pixels then difference value from two consecutive pixels is obtained [11][12]. A small difference value can be located on a smooth area and the large one is located on an edged area.

Copyright © 2012 MECS

Pixel value differencing steganography method exploits the difference value of two consecutive pixels to estimate how many secret bits will be embedded into the two pixels. Pixels located in the edge areas are embedded by a *K*-bit least-significant-bit (LSB) substitution method with a larger value of *K* than that of the pixels located in smooth areas [8]. The range of difference values is adaptively divided into lower level, middle level, and higher level. For any pair of consecutive pixels, both pixels are embedded by the *K*-bit bit least-significant-bit substitution method. However, the value *K* is adaptive and is decided by the level which the difference value belongs to. In steganographic method, a grey-valued cover image is partitioned into non-overlapping blocks of two consecutive pixels, states p_i and p_{i+1}. From each block we can obtain a different value d_i by subtracting p_i from $p_{i+1.}$ All possible different values of d_i range from -255 to 255, then $|d_i|$ ranges from 0 to 255. Therefore, the pixel p_i and p_{i+1} is located within the smooth area when the value $|d_i|$ is smaller and will hide less secret data. Otherwise, it is located on the edged area and embeds more data. From the aspect of human vision it has a larger tolerance that embeds more data into edge areas than smooth areas. PVD and *K*-bit LSB replacement method provides larger embedding capacity and higher image quality.

Advantages of using PVD and K-bit LSB Steganography

1) Gives high data embedding capacity.
2) Provides high and imperceptible quality stego images.
3) Provides high security.

III. PROPOSED SYSTEM

The objective of the proposed scheme is to design high security model for security of secret data. In this age of universal electronic connectivity, of viruses and hackers, of electronic eavesdropping and electronic fraud, there is indeed a need to protect information from passing before curious eyes or, more importantly, from falling into wrong hands. To secure information against security breaches and attacks there is need of more sophisticated techniques of protecting secret data. To avoid the problem of unauthorized data access steganography along with cryptography is the right most solution.

In proposed system cryptographic and steganographic security is combined to give two tier security to secret data. First important message is encrypted by using advance encrypted standard (AES) encryption algorithm. Then encrypted message is embedded into cover image by using PVD steganography and K-bit LSB substitution method. A block diagram of proposed system for data embedding is shown in Figure 1.

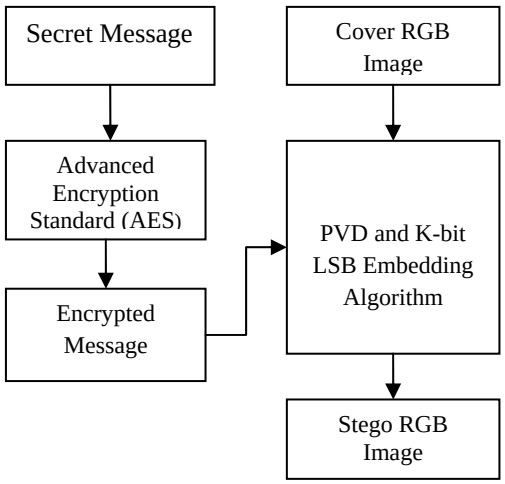


Figure 1. Proposed Message Embedding Procedure

A true color red-green-blue (RGB) image is represented as a three-dimensional $M \times N \times 3$ double matrix[13][14]. Each pixel has red, green, blue components along the third dimension with values in [0,1]. The color of each pixel in an RGB digital image is determined by the tonal value (0-255) assigned to each color channel RED, GREEN and BLUE for each pixel. In cases requiring color, an RGB color image can be decomposed and handled as three separate grayscale images.

Copyright © 2012 MECS

Secret Message is encrypted by advance encrypted standard (AES) before embedded it into cover image.

A. Embedding Algorithm

Inputs : Encrypted Secret Data(D), Cover Image(C)
Output: Stego image(S) with secret data embedded in it.

1) Divide encrypted secret data into three Data blocks D1,D2, D3.
2) Convert the each Secret Data blocks (D1,D2,D3) into binary format.
3) Split the cover image C into Red,Green and Blue Planes.(R,G and B respectively)
4) Divide Red (R) Plane of cover image into non overlapping blocks of two consecutive pixels.
5) Call PVD and K-bit LSB algorithm to embed encrypted secret data block D1 into Red Plane(R) of cover image.
6) Call PVD and K-bit LSB algorithm to embed encrypted secret data block D2 into Blue Plane(B) of cover image.
7) Call PVD and K-bit LSB algorithm to embed encrypted secret data block D3 into Green Plane(G) of cover image
8) Store the resulting image as Stego Image (S)

Block diagram of proposed system for data extraction is shown in Figure 2.

B. Data Extraction algorithm

Input : Stego Image(S)
Output:Secret Data (D)

1) Split the stego image S into Red,Green and Blue Planes.(R,G and B respectively).
2) Call PVD and K-bit LSB data extraction algorithm to extract encrypted secret data block D1 from Red Plane(R) of Stego image.
3) Call PVD and K-bit LSB data extraction algorithm to extract encrypted secret data block D2 from Blue Plane(B) of Stego image.
4) Call PVD and K-bit LSB data extraction algorithm to extract encrypted secret data block D3 from Green Plane(G) of Stego image.
5) Concate secret data block D1, secret data block 2, secret data block D3 to get Secret data D.

After data extraction we get secret message which is in encrypted form. Advanced encryption standard (AES) decryption algorithm is used to decrypt message, finally we get original secret message.

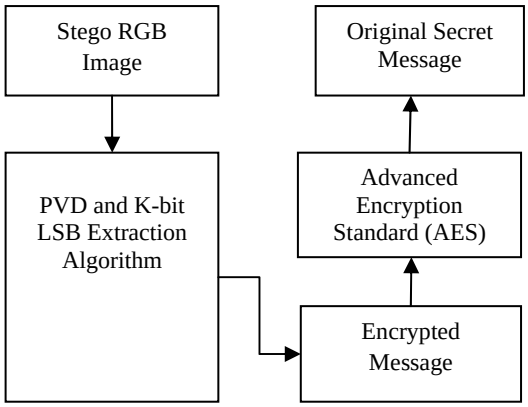


Figure 2. Proposed Message Extraction Procedure

The proposed system is highly secure since it's a combination of two highly secured techniques.

a) AES for cryptography
b) PVD and K-bit LSB Steganography

AES uses 128 bit private key which is very hard to break. PVD and K-bit LSB steganography is secured data embedding scheme. If intruder detect the partial part of the hidden message from the stego image it will be totally meaningless for him and moreover until he decrypt the message with 128 bit private key of AES which is very hard to break. To get the original secret message is impossible for intruder.

Copyright © 2012 MECS

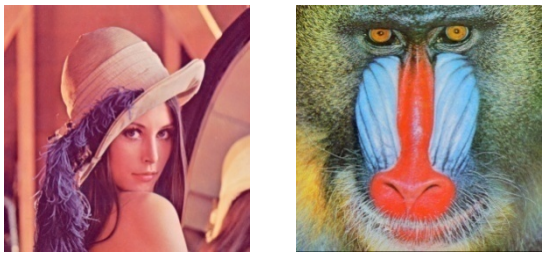
IV. EXPERIMENTAL RESULTS

The proposed High secured system using cryptography and steganography is tested by taking encrypted message and hiding them in truecolor RGB images. Nine truecolor RGB cover images with size 512×512 pixels and 24 bits per pixel are used in the experiments, and two of them are shown in Figure 3. Cover images used in experiment are Lena, Baboon, Peppers, Airplane, Barbara, Boat, Zelda, Toys, Goldhill.

All images used have Microsoft bitmap image format. Comparing restoration results requires a measure of image quality. Two commonly used measures are Mean-Squared Error and Peak Signal-to-Noise Ratio. PSNR is measured in decibels (dB). The PSNR measure is also not ideal, but is in common use. PSNR is a good measure for comparing cover image and stego image. Larger PSNR values signify better signal restoration. We use the peak signal-to-noise ratio (PSNR) to evaluate qualities of the stegoimages.

(a) (b)

Figure 3. Two RGB Cover Images (a) Lena.(b) Baboon.



(a) (b)

Figure 4. Two Stego images Created by our approach (a) Lena (embedded data are 17,45260 bits, PSNR is 39.40). (b) Baboon (embedded data are 16,56,789 bits PSNR is 35.25).

The embedding capacity is measured in terms of bits. The proposed method gives high PSNR for high capacity PVD and K-bit LSB steganography. The result of the implemented technique shows higher PSNR values, especially for high capacity steganography. The implemented method gives the highest PSNR for each image.

TABLE I, RESULTS OF CAPACITIES AND PSNR

Cover Images	**Capacity (in bits)**	**PSNR (in dB)**
Lena	20,45,260	42.40
Baboon	19,56,789	38.25
Peppers	21,10,148	41.99
Airplane	20,56,879	42.24
Barbara	19,47,628	38.57
Boat	20,46,290	41.08
Zelda	20,46,647	43.35
Toys	21,37,260	43.96
Goldhill	21,25,457	42.41
Average	20,52,484	42.41

Experiment results of two stego images are shown in Figure 4. The results that are obtained from these experiments are summarized in Table-1. From Table I, we can see that our approach results in not only more capacity but also better quality.

SUMMAY AND CONCLUSION

Security is very important for efficient communications. Cryptography and steganography are two major branches of data security. In this proposed system cryptographic and steganographic security is combined to give two tier security to secret data. In proposed scheme secret message is encrypted before hiding it into the cover image which gives high security to secret data. Advanced encryption standard (AES) is used to encrypt secret Message and PVD and *K*-bit LSB substitution method is used to hide encrypted secret message into cover image. Pixels located in edge areas

Copyright © 2012 MECS

are embedded by K -bit LSB substitution method with a larger value of K than that of the pixels located in smooth areas. Proposed approach majors in more significant promotion in the terms of adaptability, capacity, and imperceptivity. Experimental results show that proposed approach obtains both larger capacity and higher image quality. Finally we can conclude that the proposed technique is effective for secret data communication.

REFERENCES

[1] Menezes, Alfred , Paul C van Oorschot ,Scott A. Vanstone, " *Handbook of Applied Cryptography*. CRC Press", October 1996 , ISBN 0-8493-8523-7.

[2] William Stallings, "Cryptography and Network Security: Principles and practices", Pearson education, Third Edition, ISBN 81-7808-902-5.

[3] N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography," *IEEE Security and Privacy Mag."*, 2003, vol. 1, no. 3, pp. 32–44,.

[4] C. K. Chan and L. M. Chen, "Hiding data in images by simple LSB substitution," *Pattern Recognit.*, vol. 37, no. 3, pp. 469–474, 2004.

[5] R. R. Anderson and F. A. P. Peticolas, "On the limits steganography," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 4, pp. 474–481, May 1998.

[6] Joan Daemen, Vincent Rijmen, "The Design of Rijndael: AES - The Advanced Encryption Standard." *in Springer, 2002* ,ISBN 3-540-42580-2.

[7] Christof Paar, Jan Pelzl, "The Advanced Encryption Standard" *Textbook for Students and Practitioners.*

[8] Cheng-Hsing Yang, Chi-Yao Weng, Shiuh-Jeng Wang , Hun Min Sun ,"Adaptive Data Hiding in Edge Areas of Images With Spatial LSB Domain Systems", in *IEEE Information Transactions On Forensics And Security*, September 2008 , Vol. 3, No. 3.

[9] D. W. Bender, N. M. Gruhl, and A. Lu, "Techniques for data hiding," *IBM Syst. J.*, vol. 35, pp. 313–316, 1996.

[10] Data Encryption Standard (DES)'.National Bureau of Standards (US).Federal Information Processing Standards Publication National Technical Information Service. Springfield VA. April 1997.

[11] D. C. Wu and W. H. Tsai, "A steganographic method for images by pixel-value differencing," *Pattern Recognit. Lett.*, vol. 24, no. 9–10, pp. 1613–1626, 2003.

[12] H. C. Wu, N. I. Wu, C. S. Tsai, and M. S. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods," *Proc. Inst. Elect. Eng., Vis. Image Signal Process.*, vol. 152, no. 5, pp. 611–615, 2005.

[13] Rafael C. Gonzalz and Richard E. Woods, "Digital Image Processing", Pearsion Education, Second Edition, ISBN 81-7758-168-6.

[14] Rafael C. Gonzalz, Richard E. Woods and Steven L. Eddins, "Digital ImageProcessingUsing MATLAB", Pearson Education, First Indian Reprint 2004, ISBN 81-297-0515-X.

[15] Jamil, T., "Steganography: The art of hiding information is plain sight", IEEE Potentials, 18:01, 1999

[16] Stefan Katznbeisser, Fabien.A., P.Petitcolas editors, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Boston. London, 2000.

[17] Marvel, L.M., Boncelet Jr., C.G. & Retter, C., "Spread Spectrum Steganography", IEEE Transactions on image processing, 8:08, 1999

[18] Dunbar, B., "Steganography techniques and their use in an Open-Systems environment", SANS Institute, January 2002

[19] Bender, W., Gruhl, D., Morimoto, N. & Lu, A., "Techniques for data hiding", IBM Systems Journal, Vol 35, 1996

Phad Vitthal Suryakant received the Bachelor degree in Information Technology and Master degree in Computer Science and engineering from Swami Ramanand Teerth Marathwada University, Nanded, M.S.,India in 2006 and 2011 respectively. He is faculty at the Department of Computer Engineering, Pravara Rural college Engineering Loni, M.S., India.

His research areas lie in the area of Network Security, Digital Image Processing and Data Mining.

Bhosale Rajkumar Shankarrao received the Master degree in Computer Science and engineering from Swami Ramanand Teerth Marathwada University Nanded, M.S.,India in Aug 2007. Currently he is working as an Assistant Professor and Head at Pravara Rural college Engineering, Loni, M.S., India from July 2004.

His research interests include Machine Learning Network Security and Digital Image Processing.

Panhalkar Arahana Ramkisanrao received the Master degree in Computer Science and engineering from Swami Ramanand Teerth Marathwada University Nanded, M.S.,India in Aug 2008. Currently he is working as an Assistant Professor at Pravara Rural college Engineering,Loni, M.S., India from July 2004.

Her research interests include Digital Image Processing, Network Security and Machine Learning.

Copyright © 2012 MECS